Lenovo and Veeam: AI, Modern Data Resilience, Cyber Recovery, Hybrid Cloud and Infrastructure modernization

Positioning Information

Executive Summary

The power of the alliance

Enterprises are modernizing infrastructure while protecting growing volumes of data across virtual, physical, Kubernetes, SaaS, cloud, and AI-powered environments. At the same time, virtualization strategies are changing and cyber threats are moving faster, creating a fundamental business question: if disruption occurs, can critical operations recover?

Lenovo leads the infrastructure response with validated compute, enterprise storage, AI platforms, tape, services, and faster deployment paths. Veeam extends that Lenovo foundation with data resilience capabilities that help organizations protect, move, store, and recover data across changing environments.

For more than seven years, Lenovo and Veeam have worked together to simplify data protection and support resilient infrastructure transformation across core data centers, hybrid cloud, virtualization, Microsoft 365, Kubernetes, and AI. Lenovo Top Choice Express and solution-specific DCSC SIDs provide pre-defined, ready-to-go configurations that can help shorten the path from design to deployment.

Why the threat model is changing

Cyber threats are evolving alongside enterprise infrastructure. Attackers continue to target backup environments, while AI-assisted techniques can accelerate established intrusion methods and increase the speed of malicious activity. Veeam research found that 89% of threat actors targeted backup repositories, reinforcing why prevention alone is not enough. Recent public disclosures also show how AI can increase the scale and autonomy of malicious operations. Anthropic reported disrupting an AI-orchestrated cyber espionage campaign, while OpenAI documented efforts to disrupt malicious uses of AI. Together, these examples strengthen the architectural case for separation, immutability, appropriate retention, and verified recovery.

STRATEGIC TAKEAWAY: Modernization and cybersecurity strategies should include recovery from the beginning, not as a control added after deployment.

Alliance journey and commitment

Lenovo continuously invests in validation and certification to give customers broad infrastructure choice. The joint portfolio includes **49 Veeam Ready certifications** and published guidance across servers, ThinkAgile systems, ThinkSystem DM, ThinkSystem DG and ThinkSystem DE storage, AI environments, repositories, and long-term retention.

Customers can also simplify deployment and procurement through eligible Lenovo Top Choice Express configurations and DCSC SIDs. Rather than positioning these programs as guarantees, the alliance uses validated designs and pre-defined configurations to reduce design effort, improve consistency, and support a faster route to implementation.

Four pillars for modern data resilience

The Lenovo and Veeam alliance is organized around four customer priorities. Each pillar begins with a business or infrastructure challenge, then shows how Lenovo leads the platform response and how Veeam enriches it with protection, portability, and recovery capabilities.

Pillar 1: Data portability and IT modernization

Infrastructure modernization creates a difficult question for IT leaders: how can the organization evolve platforms, hypervisors, storage, and cloud strategies without creating a protection gap or limiting future choice? Lenovo provides flexible modernization pathways through ThinkSystem, ThinkAgile, storage, and services, while Veeam helps preserve protection, recovery, and workload portability during change.

Supporting virtualization change

Virtualization market changes are prompting organizations to reassess their infrastructure strategies. Some are evaluating alternative hypervisors, mixed environments, containers, or Kubernetes while continuing to support existing workloads. These transitions create both migration and resilience considerations: how can organizations move workloads while maintaining protection, recoverability, and operational continuity? Lenovo ThinkAgile and ThinkSystem platforms provide infrastructure choice, Lenovo Lifecycle and Migration Services support the transition, and Veeam helps protect data before, during, and after workload movement.

Table 1. Modernization phase and Customer Objectives

Modernization Phase	Customer Objective	Lenovo Contribution	Veeam Contribution
Before Modernization	Build a modernization strategy with flexibility to support future infrastructure decisions	ThinkAgile HX, VX, MX and FX provides a pathway for organizations evaluating modern infrastructure options, while ThinkSystem and ThinkAgile platforms create a trusted foundation for future growth.	Veeam helps establish a resilient baseline by protecting critical workloads and preserving data portability before transformation begins.
During Modernization	Reduce risk while moving workloads, refreshing infrastructure, or evolving virtualization strategies	Lenovo Lifecycle and Migration Services help organizations execute platform transitions, infrastructure refresh, and modernization projects. Top Choice Express can help accelerate delivery once the target architecture is selected.	Veeam supports workload mobility and data portability, helping protect applications and data throughout the migration process.
After Modernization	Operate the new environment with confidence while maintaining resilience and business continuity	Lenovo infrastructure, storage, and validated solutions provide the foundation for long-term operational stability and scalability.	Veeam delivers recovery, protection, hybrid cloud support, and workload portability across the new environment.
Cyberattack or Disruption	Recover business operations quickly and minimize operational impact	Lenovo combines cyber-resilient infrastructure, management capabilities, secure repository architectures, long-term retention, and validated designs to support operational continuity.	Veeam enables clean recovery, immutable protection strategies, and flexible recovery options to help restore operations with confidence.

STRATEGIC TAKEAWAY: Modernization should connect infrastructure choice, migration planning, and resilience so protection and recovery remain part of the transition.

Pillar 2: Modern data resilience

Modern data resilience requires more than backup software. It requires infrastructure that can run critical workloads, store and isolate recovery copies, support performance and retention objectives, and provide a dependable foundation for recovery. Lenovo delivers that foundation across compute, storage, hybrid cloud, end-user environments, and AI, while Veeam extends protection and recovery across the workloads and services customers depend on.

Core Lenovo + Veeam resilience components

Veeam Data Platform: Foundation for protecting and recovering physical, virtual, cloud, application, and modern workloads on Lenovo ThinkSystem, ThinkAgile, and storage platforms.

Why Lenovo: Lenovo provides the infrastructure underneath the resilience strategy,

combining ThinkSystem compute with ThinkSystem DM, DG, and DE storage options to build primary and secondary repository architectures aligned with performance, capacity, retention, and recovery requirements. Lenovo validated designs and Veeam Ready certifications help translate those requirements into deployable architectures.

Veeam Data Cloud: Cloud-based resilience capabilities that complement Lenovo-led infrastructure and hybrid cloud strategies.

Why Lenovo: It extends a Lenovo-led hybrid infrastructure strategy with cloud-based protection, allowing customers to combine on-premises Lenovo infrastructure with Veeam-managed cloud resilience rather than treating cloud protection as a separate architecture.

Microsoft 365 protection: Recovery flexibility and retention for Exchange, SharePoint, OneDrive, and Teams, complementing Lenovo end-user and infrastructure environments.

Why Lenovo: Lenovo connects the digital workplace with the broader infrastructure strategy, extending the resilience conversation from user devices and collaboration services to the data center. Veeam protection for Microsoft 365 helps safeguard the business data created across Exchange, SharePoint, OneDrive, and Teams.

Veeam Vault: An additional off-site cloud copy for selected retention, immutability, and geographic separation requirements.

Why Lenovo: It complements Lenovo repository and Lenovo Tape architectures with an additional cloud-based protection layer, giving customers more flexibility when designing 3-2-1-1-0 strategies across on-premises, offline, and cloud tiers.

Veeam Kasten: Application-aware protection, recovery, and mobility for Kubernetes and cloud-native workloads, including Lenovo AI Factory environments.

Why Lenovo: Lenovo Hybrid AI Factory, ThinkSystem, ThinkAgile, and storage provide the infrastructure foundation for modern Kubernetes and AI environments, while Kasten adds application-centric protection and mobility. This makes resilience part of the platform architecture as AI workloads move into production.

Lenovo deployment advantage: Lenovo Top Choice Express and solution-specific DCSC SIDs make the alliance easier to consume. Pre-defined configurations reduce repeated design work, help identify the Lenovo infrastructure required for the solution, and accelerate the path from sizing and quoting to ordering and deployment.

STRATEGIC TAKEAWAY: Lenovo turns data resilience into an infrastructure strategy, with Veeam extending protection across the workloads and services customers depend on.

Pillar 3: Cyber resilience with 3-2-1-1-0

The 3-2-1-1-0 approach gives organizations a practical framework for resilient backup: three copies of data, on two media types, with one off-site copy, one offline or immutable copy, and zero recovery errors through verification. Lenovo and Veeam make the framework tangible through infrastructure, storage, tape, software, and recovery practices.

Table 2. The 3-2-1-1-0 approach

Principle	Lenovo + Veeam example
3 copies	Production data plus primary and secondary recovery copies
2 media types	ThinkSystem DM, ThinkSystem DG, or ThinkSystem DE storage combined with another repository or Lenovo Tape
1 off-site	A geographically separated Lenovo environment or Veeam Vault

Principle	Lenovo + Veeam example
1 offline or immutable	Lenovo Tape for physical air gap or immutable repository options supported by the selected architecture
0 errors	Verified restore processes and recovery testing with Veeam capabilities

A practical recovery architecture.

Table 3. Resilience and Data layer

Resilience Layer	Data Layer	Business Challenge	How Lenovo Helps	How Veeam Helps
Mission-critical applications and business workloads	Production Data	Organizations need reliable platforms for critical applications while maintaining continuity and performance.	ThinkSystem and ThinkAgile provide a trusted infrastructure foundation for enterprise workloads, modernization, and growth.	Veeam protects production workloads and helps keep recovery options available when disruptions occur.
Copy #1: First recovery layer for operational restores, fast recovery, and day-to-day protection	Primary Repository	Enterprises need a secure and efficient location for protected data that supports recovery objectives and growth.	ThinkSystem DM and ThinkSystem DG provide enterprise storage designed for availability, scalability, and repository performance.	Veeam Data Platform manages backup, recovery, immutability, and data resilience operations across the repository layer.
Copy #2: Additional protection against infrastructure failures, corruption, or ransomware	Secondary Repository	Organizations need additional protection layers to reduce the impact of operational failures, ransomware, or site-level disruptions.	ThinkSystem DM, ThinkSystem DG, and ThinkSystem DE create secondary protection layers aligned to business, performance, and budget requirements.	Veeam Backup Copy, immutability strategies, and secondary recovery workflows help improve resilience and recovery confidence.
Copy #3: Air-gapped retention for long-term preservation and cyber resilience	Long-Term Retention	Regulatory, governance, and business requirements can demand retention beyond operational backup windows.	Lenovo Tape provides a cost-effective, secure air-gapped retention layer for long-term preservation.	Veeam helps manage retention policies, recovery access, and long-term protection strategies across retained data.
Optional Off-Site Layer: Geographic separation when required	Optional Off-site Copy	Some organizations require an additional off-site layer to strengthen resilience and disaster recovery objectives.	Lenovo infrastructure can extend into hybrid environments while maintaining operational consistency.	Veeam Vault provides an optional cloud-based protection layer within a broader resilience strategy.

STRATEGIC TAKEAWAY: Cyber resilience is stronger when recovery copies are separated, protected, retained appropriately, and tested instead of merely created.

Pillar 4: AI resilience

As AI initiatives evolve from experimentation to business-critical services, organizations face a new challenge: ensuring that the data, models, pipelines, and applications powering those initiatives remain protected, recoverable, and available. According to Lenovo CIO Playbook 2026, 27% of organizations investing in AI report a well-established data governance and security strategy, 56% are still developing their approach, and 15% describe current controls as largely ad hoc.

- AI changes both the attack surface and the speed of response

- Lenovo Hybrid AI Factory

AI changes both the attack surface and the speed of response

Through 2025 and 2026, the risk profile around enterprise AI moved from speculative to documented. Anthropic reported that a state-sponsored group used Claude Code, orchestrated through the Model Context Protocol, in an espionage campaign against roughly 30 organizations. Anthropic estimated that the agent performed 80% to 90% of the tactical work, with activity reaching thousands of requests and often several requests per second.

OpenAI threat reporting describes more than 40 disrupted networks and a recurring pattern of adversaries using AI to accelerate established playbooks. 89% of threat actors specifically target an organization's backups. Together, these signals reinforce the need for separated recovery copies, immutability, retention that accounts for delayed detection, and restores that are tested rather than assumed.

Table 4. Public threat signals that explain why AI resilience requires isolated recovery, immutability, appropriate retention, and verified restores

Market Signal	What Happened	What It Means for the Lenovo + Veeam Conversation
Mission-critical applications and business workloads	Production Data	Organizations need reliable platforms for critical applications while maintaining continuity and performance.
Copy #1: First recovery layer for operational restores, fast recovery, and day-to-day protection	Primary Repository	Enterprises need a secure and efficient location for protected data that supports recovery objectives and growth.
Copy #2: Additional protection against infrastructure failures, corruption, or ransomware	Secondary Repository	Organizations need additional protection layers to reduce the impact of operational failures, ransomware, or site-level disruptions.
Copy #3: Air-gapped retention for long-term preservation and cyber resilience	Long-Term Retention	Regulatory, governance, and business requirements can demand retention beyond operational backup windows.
Optional Off-Site Layer: Geographic separation when required	Optional Off-site Copy	Some organizations require an additional off-site layer to strengthen resilience and disaster recovery objectives.

Lenovo Hybrid AI Factory

Lenovo Hybrid AI Factory provides the infrastructure foundation for enterprise AI through Lenovo ThinkSystem compute, ThinkAgile solutions, and ThinkSystem storage. Veeam Kasten adds policy-driven, application-aware protection and mobility for Kubernetes-based AI services. Together, they help build resilience into the AI platform before models, data pipelines, and applications become business-critical.

Lenovo infrastructure and Veeam Kasten address complementary AI resilience requirements, from operating AI as a production service to protecting complete applications, data pipelines, and recovery workflows.

Table 5. Enterprise AI resilience objectives and the complementary roles of Lenovo infrastructure

and Veeam Kasten

Enterprise AI Objective	Why It Matters	Lenovo Contribution	Veeam Contribution
Operate AI as a production business service	As AI moves from pilots to critical operations, downtime, data loss, and failed recoveries can affect business outcomes.	Lenovo Hybrid AI Factory provides a validated enterprise AI architecture designed for scalable and reliable deployments.	Veeam Kasten helps protect AI applications, Kubernetes resources, and application state through policy-driven resilience workflows.
Protect complete AI pipelines, not individual components	AI workloads depend on models, datasets, vector databases, metadata, and application state that must be recovered consistently together.	Lenovo Hybrid AI Factory combines compute, networking, and enterprise storage into a unified AI platform.	Veeam Kasten provides application-centric protection designed to recover complete AI services and pipelines rather than isolated volumes or containers.
Reduce AI downtime and recovery complexity	Long recovery windows can disrupt inference services, AI applications, and revenue-generating workloads.	Lenovo ThinkSystem DM provides high-performance recovery tiers for critical AI data and services.	Veeam Kasten enables policy-driven recovery, application awareness, and automated recovery workflows.
Protect high-value AI assets from cyber threats	Models, enterprise data, embeddings, and vector databases are valuable targets for ransomware and malicious deletion.	Lenovo provides secure AI infrastructure, resilient ThinkSystem storage, and validated architectures designed to strengthen operational continuity.	Veeam Kasten provides immutable recovery points, security controls, policy-driven protection, and isolated recovery workflows.
Scale AI confidently	AI environments need to grow without increasing operational complexity or introducing recovery risk.	Lenovo Hybrid AI Factory scales from initial configurations to larger deployments while maintaining architectural consistency.	Veeam Kasten scales protection, application mobility, and recovery policies as AI environments expand across clusters and platforms.

STRATEGIC TAKEAWAY: AI resilience should protect the full application and data chain, with recovery designed into the platform from day one.

Coordinated services and modernization support

Modernization initiatives involve more than deploying infrastructure. Organizations must balance business continuity, application dependencies, recovery objectives, migration timelines, and operational risk while evolving their environments. Coordinated services and support therefore belong in the alliance story and create a natural foundation for a future dedicated services module.

Lenovo Lifecycle and Migration Services can help organizations assess, plan, deploy, and transition to new environments, while Veeam helps preserve protection, workload portability, and recovery readiness throughout the transformation. Together, the approach keeps migration and resilience connected from planning through operational handoff.

- From validated design to faster deployment
- Examples of the alliance in action

From validated design to faster deployment

Top Choice Express is a central Lenovo differentiator for Veeam-based data protection solutions. Eligible configurations use pre-defined building blocks and solution-specific DCSC SIDs to reduce configuration effort and help accelerate quoting, ordering, and deployment.

The combination of Lenovo Press guidance, Veeam Ready certifications, DCSC SIDs, and Top Choice Express helps customers and sellers move from architecture to implementation with greater consistency. Availability, delivery, and specific configurations should always be confirmed for the customer's geography and requirements.

Examples of the alliance in action

Examples of the alliance in action Customer examples demonstrate how Lenovo infrastructure and Veeam data resilience capabilities can address operational continuity, cyber recovery, Kubernetes protection, and hybrid cloud requirements.

24/7 manufacturing and cyber recovery

A global manufacturer operating 20 facilities across more than ten countries reported completing recovery from a cyberattack in four hours with zero data loss using Veeam Data Platform and Veeam Data Cloud Vault. Before the change, SAP ERP backups could take approximately 72 hours and recovery attempts had failed.

Lenovo + Veeam sales motion: Lead with the business cost of halted production, missed deliveries, and supply-chain disruption. Position Lenovo ThinkSystem compute and ThinkSystem storage as the resilient on-premises foundation, Veeam Data Platform for workload protection and recovery, and Veeam Vault or Lenovo Tape for an isolated additional copy. Where eligible, use Top Choice Express and solution SIDs to accelerate the infrastructure conversation.

Kubernetes services at scale

A service provider supporting 16,000 clients described the operational burden of protecting Kubernetes applications with manually maintained scripts. Veeam Kasten was selected to automate application-centric protection across application data and configuration.

Lenovo + Veeam sales motion: Start with the application, not only the cluster. Position Lenovo ThinkSystem or Lenovo Hybrid AI Factory as the infrastructure foundation, then use Veeam Kasten to protect complete Kubernetes applications, including data, metadata, and configuration. This opens a broader discussion around application mobility, recovery automation, and AI workloads running on Kubernetes.

Cloud-first construction and critical project data

A large construction company undertaking a cloud-first transformation needed to protect critical digital assets, including building information modeling applications and drone-captured site data, while reducing the risk of costly project delays. The company selected Lenovo and Veeam to unify and simplify resilience across its evolving environment.

Lenovo + Veeam sales motion: Connect resilience to project continuity rather than backup alone. Position Lenovo infrastructure and ThinkSystem storage for dependable local performance and recovery, Veeam Data Platform for consistent protection across hybrid workloads, Veeam Data Cloud for Microsoft 365 for collaboration data, and Veeam Vault for an off-site immutable copy. Lenovo services can help coordinate the transition from legacy protection to the target architecture.

When Lenovo and Veeam may be a good fit

The alliance is particularly relevant when organizations are addressing one or more of the following priorities:

- Virtualization or hypervisor change
- Infrastructure or storage modernization
- Repository capacity expansion
- AI platforms moving toward production
- 3-2-1-1-0 or cyber recovery redesign
- Long-term retention or air-gap requirements
- Microsoft 365 or Kubernetes protection
- Faster deployment through Top Choice Express and solution SIDs

Lenovo and Veeam resources

For more information, see these resources:

- Lenovo with Veeam Data Resilience Validated Solutions for Modern Enterprises: https://lenovopress.lenovo.com/lp2419-lenovo-with-veeam-data-resilience-validated-solutions-for-modern-enterprises
- Lenovo Validated Design: AI Resilience with Veeam Kasten on Lenovo AI Factory: https://lenovopress.lenovo.com/lp2382-lenovo-validated-design-ai-resilience-with-veeam-kasten-on-lenovo-ai-factory
- Lenovo ThinkSystem DM Series: https://lenovopress.lenovo.com/lp0941-lenovo-thinksystem-dm-series-unified-storage-arrays
- Lenovo ThinkSystem DE Series: https://lenovopress.lenovo.com/lp0940-lenovo-thinksystem-de-series-storage-arrays
- Lenovo ThinkSystem storage with Veeam reference architecture: https://lenovopress.lenovo.com/lp1769-reference-architecture-backup-solution-with-thinksystem-storage-and-veeam
- Lenovo Tape Solutions: https://lenovopress.lenovo.com/storage/tape/library
- Lenovo Hybrid AI Factory: https://lenovopress.lenovo.com/servers/hybrid-ai-factory#sort=relevance
- Veeam Data Platform: https://www.veeam.com/products/veeam-data-platform.html
- Veeam Kasten for Kubernetes data protection: https://www.veeam.com/products/cloud/kubernetes-data-protection.html
- Veeam report on cyberattacks and backup targeting: https://www.veeam.com/company/press-release/veeam-report-finds-close-to-70-percent-of-organizations-still-under-cyber-attack-despite-improved-defenses.html

External References

For more information, see these resources:

- Anthropic: Disrupting AI espionage: https://www.anthropic.com/news/disrupting-AI-espionage
- OpenAI: Disrupting malicious uses of AI: https://openai.com/index/disrupting-malicious-ai-uses/

Solution Design Considerations and Disclaimers

All solution designs should be properly sized and validated based on the customer's workloads, capacity, performance, recovery objectives, retention requirements, data growth, and deployment architecture.

Recovery, retention, immutability, and cyber resilience capabilities vary by Lenovo platform, Veeam edition, configuration, and deployment model. Validate each design against specific customer requirements.

Products, certifications, SIDs, Top Choice Express configurations, services, and delivery programs may vary by geography and over time. Availability should be confirmed for the intended deployment.

Examples and use cases in this brief are illustrative. Customer environments, architectures, requirements, and outcomes may differ, and customer-specific claims and results should be validated.

AI resilience requires workload-specific planning across models, datasets, vector databases, metadata, Kubernetes resources, application state, governance, security controls, recovery requirements, and operational continuity.

Authors

Edgar Rodriguez is the Global Alliance Manager for Cyber Resiliency Partners at Lenovo. With over 18 years of experience in the technology sector, Edgar drives the strategic partnership between Lenovo and data protection partners. He has a customer-centric and data-driven approach to ensure our global go-to-market efforts always start with the customer, their challenges, priorities, and words. He works cross-functionally and collaboratively to craft compelling messaging, coordinate cross-organizational teams, implement best practices, to set Lenovo apart from the competition. He is passionate about understanding why people buy life-changing products and how these products get into their hands, always thinking on customer journeys, feelings, and insights.

Related product families

Product families related to this document are the following:

- Artificial Intelligence

Notices

Lenovo may not offer the products, services, or features discussed in this document in all countries. Consult your local Lenovo representative for information on the products and services currently available in your area. Any reference to a Lenovo product, program, or service is not intended to state or imply that only that Lenovo product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any Lenovo intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any other product, program, or service. Lenovo may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

Lenovo (United States), Inc.
8001 Development Drive
Morrisville, NC 27560
U.S.A.
Attention: Lenovo Director of Licensing

LENOVO PROVIDES THIS PUBLICATION ”AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. Lenovo may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

The products described in this document are not intended for use in implantation or other life support applications where malfunction may result in injury or death to persons. The information contained in this document does not affect or change Lenovo product specifications or warranties. Nothing in this document shall operate as an express or implied license or indemnity under the intellectual property rights of Lenovo or third parties. All information contained in this document was obtained in specific environments and is presented as an illustration. The result obtained in other operating environments may vary. Lenovo may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Any references in this publication to non-Lenovo Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this Lenovo product, and use of those Web sites is at your own risk. Any performance data contained herein was determined in a controlled environment. Therefore, the result obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

© Copyright Lenovo 2026. All rights reserved.

This document, LP2569, was created or updated on November 17, 2026.

Send us your comments in one of the following ways:

- Use the online Contact us review form found at:
  https://lenovopress.lenovo.com/LP2569
- Send your comments in an e-mail to:
  comments@lenovopress.com

This document is available online at https://lenovopress.lenovo.com/LP2569.

Trademarks

Lenovo and the Lenovo logo are trademarks or registered trademarks of Lenovo in the United States, other countries, or both. A current list of Lenovo trademarks is available on the Web at https://www.lenovo.com/us/en/legal/copytrade/.

The following terms are trademarks of Lenovo in the United States, other countries, or both:
Lenovo®
ThinkAgile®
ThinkSystem®

The following terms are trademarks of other companies:

Microsoft®, Microsoft 365®, OneDrive®, and SharePoint® are trademarks of Microsoft Corporation in the United States, other countries, or both.

Other company, product, or service names may be trademarks or service marks of others.